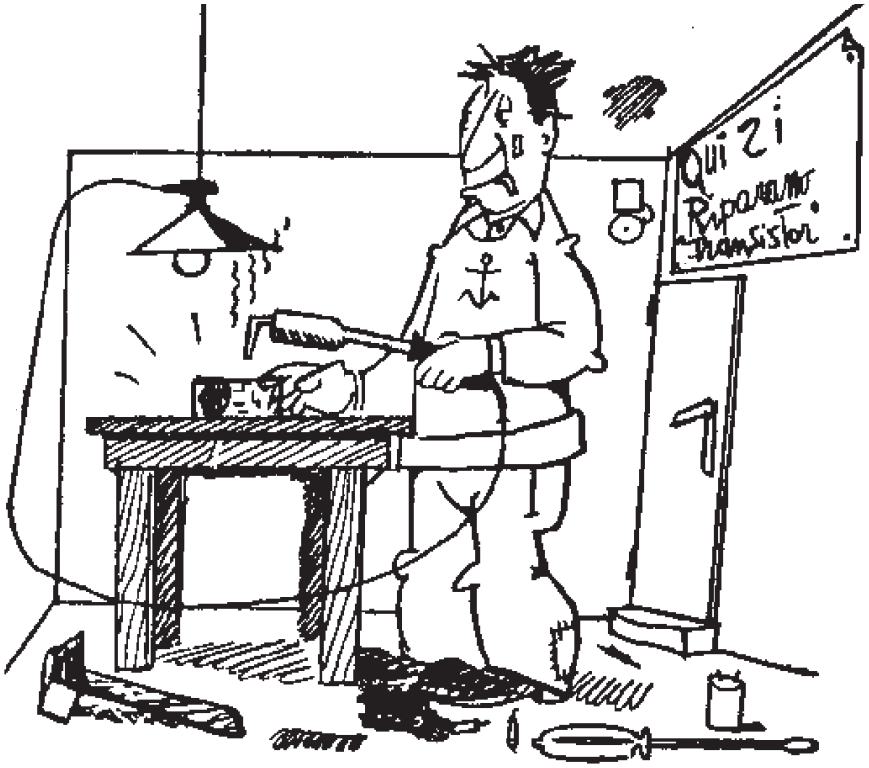


Questo articolo è stato pubblicato su....

ELETTRONICA FLASH

CELLULARE & PC

NET MONITOR NOKIA

Daniele Cappa IW1AXR

Due parole per cercare di capire qualche cosa di più circa il NetWork Monitor che il programma Logo Manager ha attivato sul nostro cellulare Nokia 51xx e 61xx.

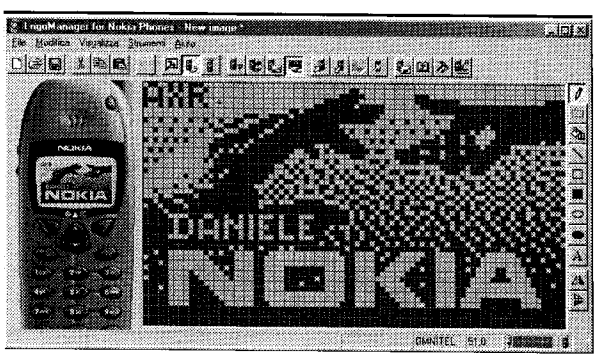
Sono necessarie alcune premesse: il programma LogoManager è reperibile presso l'indirizzo www.logomanager.co.uk, l'autore è Mike Bradley di Belfast.

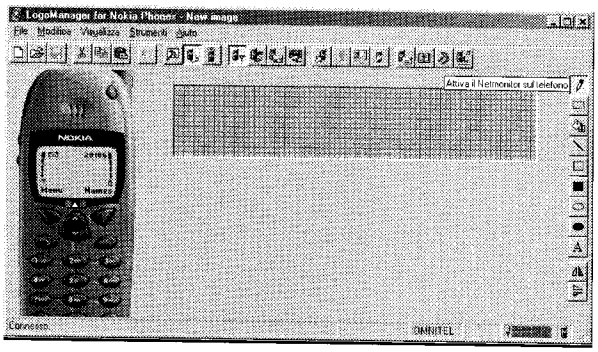
È necessario collegare il telefono al PC tramite una interfaccia Nokia Data Suite, o cavo compatibile come da me illustrato sulle pagine di E.F. n°192 - marzo 2000.

Il Netmonitor del telefono è attivato da una opzione del programma citato, l'attivazione avviene anche con la versione dimostrativa, e consente di curiosare nel telefono in modo molto approfondito leggendo i dati sia comodamente seduti in poltrona tramite il monitor del PC, sia direttamente sul display del telefono entrando nel menù che il mio 6150 vede come numero 12 ora presente sul cellulare.

Sono forniti parametri di rete, canali, potenza, distanza, intensità dei segnali ricevuti fino a nove celle contemporaneamente, le condizioni di carica della batteria sono molto dettagliate.

Il programma non permette di recare danni sul telefono, è in ogni modo bene astenersi dal compiere operazioni azzardate!





L'attivazione del menu avviene con il programma citato e resta disponibile anche quando cavo e interfaccia Nokia non sono più collegate, per accedervi è necessario premere il tasto MENU, cercare la nuova voce NET MONITOR, quindi selezionarla con il tasto sinistro. Ora è necessario scegliere il numero che identifica il menù che desideriamo vedere. In queste condizioni abbiamo attivato il "Field Test Display" in "Data Display Mode" che sarà la nostra finestra all'interno del telefono.

Esistono altri due modi di funzionamento, il modo Help che si attiva e disattiva premendo per un paio di secondi il tasto * (asterisco) partendo dal Data Display Mode e fornisce un aiuto simile a quanto vedremo tra poco nelle tabelle di sinistra.

La terza possibilità è fornita dal "Execute Mode", l'accesso avviene partendo sempre dal Data Display Mode eseguendo la sequenza MENU, NETMONITOR, SELEZIONA, OK.

Su alcuni menu questa sequenza non provoca alcun effetto, mentre su altri cambia il settaggio del telefono, ad esempio sul menu numero 45 provoca la disabilitazione della parte trasmittente del telefono, che in queste condizioni risulta essere inutilizzabile. Attenzione dunque a eseguire due volte la sequenza necessaria a entrare nel menù dove siamo già! Alcuni menù fanno capo a settaggi della SIM CARD che potrebbe non gradire la nostra intrusione.

Gli esempi sono riportati con a sinistra la schermata di aiuto, a destra quello che potremmo leggere sul telefono, o meglio quello che io ho letto sul mio 6150!

Di seguito alcune righe di info in merito.

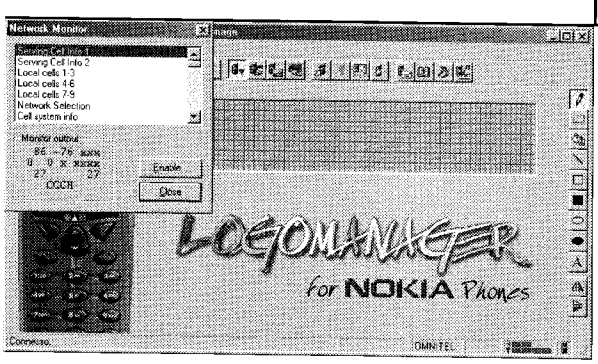
Le "videate" sul display del cellulare sono numerate da 01 a 89, non tutte sono presenti e non tutte sono riportate in questa sede che si prefigge di illustrare le cose per noi più interessanti.

È utile ricordare che alcuni valori variano molto velocemente, potrebbero essere cambiati da quando ho riportato il contenuto di una finestra e di una successiva. Il canale in uso appare molto spesso, questo potrebbe cambiare più volte nello spazio di pochi secondi.

I valori che non sono disponibili in questo momento, che possono essere valori di ricezione se il telefono non è in zona coperta dal servizio, di trasmissione se non si sta effettuando una chiamata, condizioni del caricabatterie se non è collegato al telefono, vengono visualizzati con una serie di XXXX secondo quanti sono i caratteri interessati al valore da visualizzare.

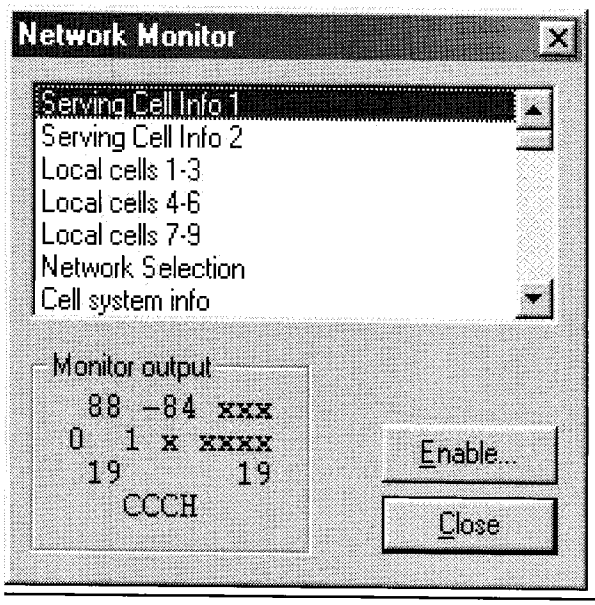
Serving Cell Info 1

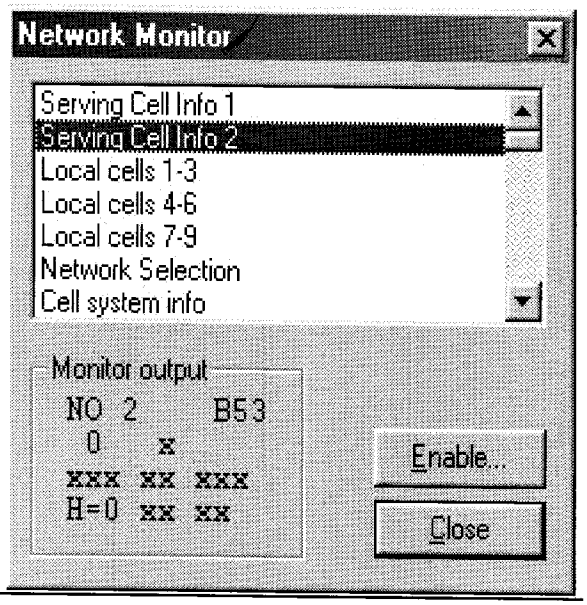
01 Ch RxLev Txpwr	01 88 -77 (*5)
Tslot Ta Rq Rlt	7 0 0 20
C1 C2 CHT	27 27 CCCH



Ch è il canale usato in quel momento, numeri compresi tra 1 e 124 sono canali GSM a 900MHz, quelli compresi tra 512 e 885 sono canali DCS a 1800MHz.

RXLev è il livello di ricezione, espresso in dBm, che il telefono riceve dalla cella in uso sul canale Ch, valori inferiori a –100dBm non sono visualizzati.





Tslot Time Slot, compreso tra 0 e 7, è l'intervallo di tempo in uso in questo istante.

Rq qualità della ricezione, compreso tra 0 e 7.

Ta Time advance, fornisce la distanza approssimativa dalla cella, Il numero letto va moltiplicato per 547 e si ottiene la distanza in metri.

Rlt Radio Link Timeout, è compreso tra 0 e 64, se il telefono è fuori copertura di rete viene visualizzato "XX".

C1 e C2 possono essere compresi tra –99 e 99 e rappresentano la perdita di qualità della tratta radio della cella in uso e della successiva miglior cella ricevibile.

CHT può assumere 23 diverse denominazioni secondo che il canale sia impegnato da traffico di tipo dati (Fnnn o Hnnn), abbia o meno un "subchannel" (THRn), stia trasmettendo il Cell Broadcast (CCHR), o non abbia copertura (NSPS).

Pm tipo di paging. NO per normale, EX per esteso, RO per riorganizzazione

Ro Roaming, è attivo quando viene visualizzata una R, significa che si sta usando una rete non propria che ci fornisce ospitalità.

Rar numero massimo di ritrasmissioni casuali.

Bsic viene visualizzata una lettera B seguita dal valore di Bsic, compreso da 0 e 63.

- I valori tra parentesi sono letti solo se il telefono sta effettuando una chiamata.

Local cell 1-3

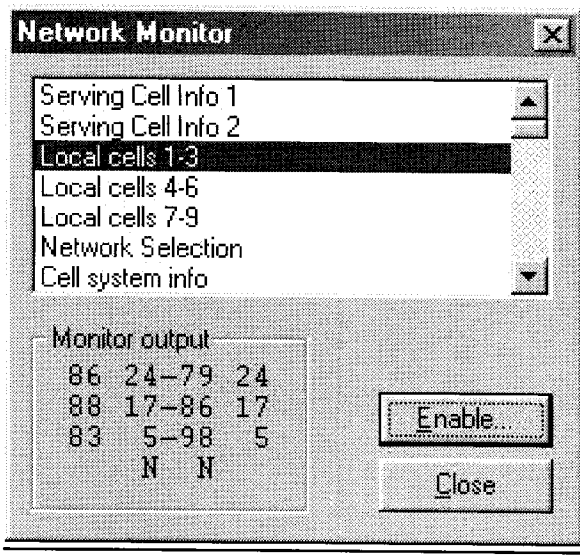
03 Sch C1 RxLev C2 1ch C1 RxLev C2 2ch C1 RxLev C2 1N 2N	03 88 30 -75 28 86 26 -80 26 118 23 -81 23 N B

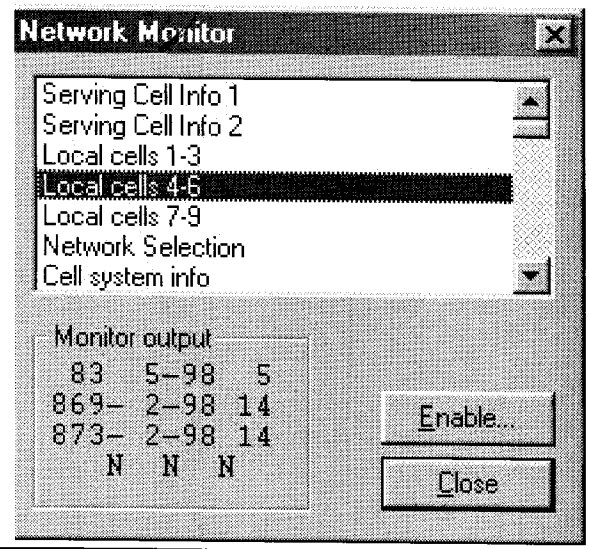
Serving Cell Info 2

02 Pm Rar Ro Bsic RelR QLF CRO To PenT H Maio Hsn	02 NO 2 B53 16 (0) xxx xx xxx H=0(H-1)(4) (23)

Local Cell 4-6

04 3ch C1 RxLev C2 4ch C1 RxLev C2 5ch C1 RxLev C2 3N 4N 5N	04 81 12 -91 13 84 6 -97 6 869- 0 -98 16 N N N





Local Cell 7-9

05 6ch C1 RxLev C2 7ch C1 Rx Lev C2 8ch C1 Rx Lev C2 6N 7N 8N	05 94 2 -99 2 xxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxx N xx xx

Network Selection

06 Lreg 1For 1Pre 2For 2Pre 3For 3Pre 4For	06 22201 22210 xxxxx 22288 xxxxx xxxxx xxxxx xxxxx

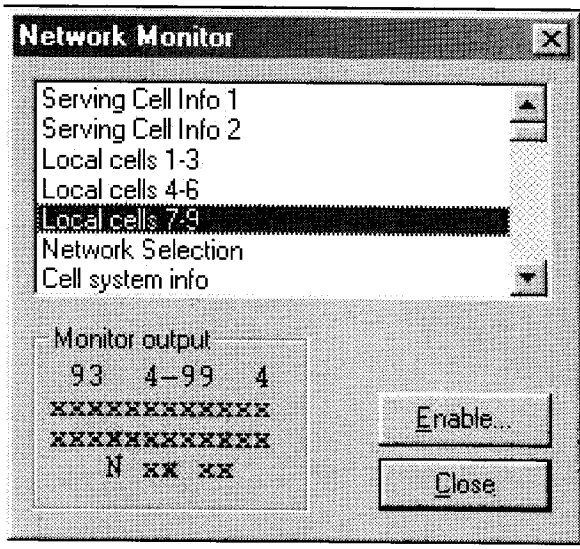
Le schermate 03, 04 e 05 evidenziano il canale in uso (Sch) e i successivi 8 canali che il telefono vede. Sono presentati in ordine decrescente del segnale (RxLev, sempre espresso in dBm) e ovviamente cambiano spesso posizione tra loro.

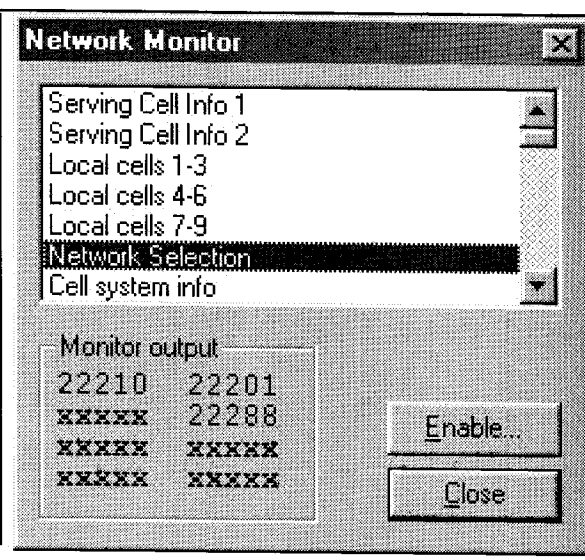
Anche in questo caso i valori inferiori a –100dBm non vengono visualizzati.

Lreg è l'ultima rete registrata, quella in uso, nell'esempio è Omnitel (22210) mentre Tim e Wind (22201 e 22288) non sono accessibili.

Notiamo che i 222 rappresentano il Network Country Code (NCC), che per l'Italia è 222.

Così come gli ultimi due numeri rappresentano l'operatore di telefonia mobile (Network Code, NC), 01 corrisponde a TIM, 10 a OMNITEL e 88 a WIND.





Cell system info

```
        07
         E A H C I   BR
         1 1 0 0 0   10
         ECSC   2Ter   MB
           1       1    1
```

Se E è a 1 sono consentite le chiamate di emergenza.

Se A è a 1 sono consentite le procedure di connessione e di disconnessione.

Se H è a 0 non è supportato l'half rate, il significato non è ben chiaro, sembra che ci sia la possibilitàdi trasmettere i pacchetti che contengono le nostre parole digitalizzate a velocità dimezzata.

I campi C, I, B e R interessano la trasmissione in broadcast, il valore 1 significa abilitazione e il valore 0 significa non abilitazione.

MB può assumere i valori: 0, 1, 2 o 3. Interessa solamente i telefoni bibanda e riporta le condizioni delle celle ricevute con segnale migliore. 0 (00) per 4 celle,3 (11) per tre celle, 2 (10) per due celle e 1 (01) per una cella. Il valore tra parentesi è in binario il che spiega come lo 00 sia in realtà il riporto da 4, in binario 100, visto su due sole cifre.

Timers

```
10                      10
 TMSI(in hex)            TMSI9686BC52
 T321:    x/xx           T321:   1/ 10
 PRP:      DSF AGC       PRP:4   22 96
           AFC   Ch              17   88
```

È una videata di timer, l'unica cosa comprensibile è il Ch, 88 ...

Network parameters

```
11                      11
MCC              MNC    CC:222  NC10
 Local Area Code           LAC:10002
 Canale di servizio        CH :    86
    Cell Id.               CID : 2233
```

MCC Mobile Country Code, come spiegato prima 222 corrisponde all'Italia.

MNC Mobile Network Code, 10 corrisponde a Omnitel.

LAC Location Area Code, in esadecimale

CH Numero del canale in uso.

CID Identificativo della cella, anche questo in esadecimale, può essere inteso come il "nome" della cella, in luoghi diversi ci potrebbero essere celle che funzionano sullo stesso canale, ma non possono esserci due celle con lo stesso nome. La rete localizza il nostro telefono dal nome della cella su cui il nostro telefono si è registrato.

I menu 12, 13, 17, 18 e 19 vengono riportati così come si leggono sul display del mio telefono....

```
12                  13                  17
CHIPER   :OFF       NOTALLOWED
HOPPING  :ON        DTX(DEF):ON         BTSTEST
DTX      :ON        DTX(BS)  :USE         OFF
IMSI     :ON
```

Interessano la possibilità che ha il telefono di spostarsi dal servizio di una cella ad un'altra, in particolare il menu 17 è possibile cambiarlo ripetendo la sequenza MENU, NETMONITOR, 17, OK, con cui si abilita il BTS TEST a ON.

In questo caso il canale in cui vogliamo far funzionare il telefono va memorizzato nella posizione di memoria numero 33 della carta SIM, cosa che non è possibile fare con il programma qui citato. La posizione 33 contiene ora uno 0 che ci impedisce di commutare il BTS TEST in ON. Questa possibilità ci permetterebbe di verificare la copertura di una singola cella semplicemente spostandoci nella sua zona. I menu che dovrebbero permetterci di curiosare nelle locazioni di memoria della SIM sono i numeri 52 e 53 che Logo Manager non ci abilita.

```
18                  19
     LIGHTS            CELL BARR
      OFF               ACCEPTED
```

Dal menu 18 è possibile accendere, e successivamente spegnere, l'illuminazione del display in modo permanente tramite la solita se-

quenza, MENU, NETMONITOR, 18, OK.

Il menu 19 invece usa la citata sequenza per commutare CELL BARR ACCEPTED in CELL BARR REVERSE e CELL BARR DISCARD, per poi iniziare da capo.

Il funzionamento normale avviene con CELL BARR ACCEPTED in cui il telefono si registra unicamente sulle celle non bloccate, mentre in REVERSE il funzionamento avviene solo sulle celle bloccate che potrebbero essere le celle in test, o comunque normalmente non disponibili.

La cosa è verificabile andando sul menu 03 e controllando che nella cella in uso, che è la prima visualizzata, ci verrà mostrato un numero di canale che prima non era presente in nessuno dei menu 03, 04 e 05.

Nel modo CELL BARR DISCARD sono accessibili sia le celle bloccate che quelle non bloccate.

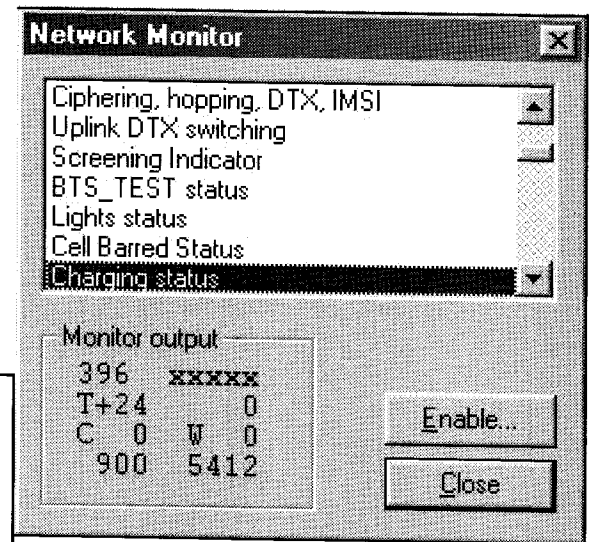
Il menu 20 è molto interessante, si tratta delle condizioni della batteria. Per questo ho aggiunto una terza finestra con i dati letti sia normalmente sia a carica batterie collegato:

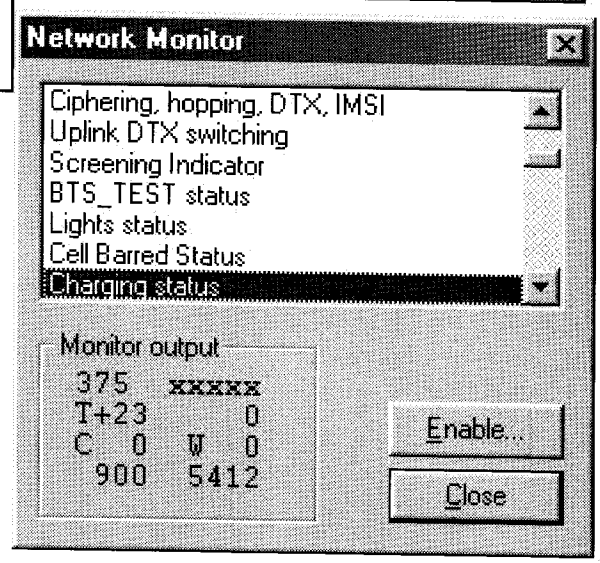
I dati cambiano sia durante la carica della batteria, sia a carica terminata e sono diversi secondo che tipo di batteria è in uso.

Charging status

20	20	20
Vbat ChMod	373 xxxxx	384 LithC
Tbat ChTime	T+26 0	T+27 2
ChrgVol PWM	C 0 W 0	C 48 W255
Btype BFDC	900 5412	900 5412
	Non in carica	In carica

Vbat	tensione della batteria, 384 corrisponde a 3.84V
Tbat	temperatura della batteria in gradi centigradi, da -30 a 90 gradi
Chrgvol	Tensione di carica della batteria, 48 corrisponde a 4.8V, valori da 0 a 18.7V
Btype	Capacità della batteria in mA.
Chtime	Tempo trascorso da che la batteria è in carica, formato HMM, il timer si azzera se viene scollegato il carica batterie
PWM	Controllo di carica, all'inizio è 255, va da 0 a 255.
BFDC	Controllo della corrente di carica, quando è a 0 la carica viene interrotta
ChMod	questo parametro comprende molte indicazioni che possono apparire sul display:
xxxxx	carica batterie non collegato o carica disabilitata
BatCk	controllo della batteria
ChaCk	controllo del carica batterie
Charg	batteria in carica
CelBr	è stato rilevato almeno un elemento della batteria difettoso, la carica è stata interrotta
CurFa	la misura della corrente del carica





	batterie è errata, la carica è stata interrotta
Faile	errore generico
InitC	inizializzazione della carica
I_Che	controllo iniziale della carica
L_Che	controllo della carica della batteria al litio
F_Che	controllo della carica veloce
M_Che	controllo della carica di mantenimento
MaBFD	carica di mantenimento BFD
LiAFu	batteria al litio carica
LiDCH	batteria al litio in carica DCH
LiHot	batteria al litio in carica veloce
LiFul	batteria al litio completamente carica
LNFTx	batteria al litio non completamente carica con telefono in trasmissione
LithC	batteria al litio in carica
LiTxO	batteria al litio in carica con telefono in trasmissione
TmpFa	il sensore della temperatura è guasto, la carica è stata interrotta
TxOnC	batteria NiMh in carica con telefono in trasmissione
VolFa	la tensione di carica misurata è errata, la carica è stata interrotta
Maint	carica di mantenimento in corso
BSlFa	carica della batteria sospesa per un guasto
FastC	carica veloce in corso
FullM	la batteria è carica, inizia ora la carica di mantenimento
HotM	la batteria è calda, inizia la carica di mantenimento
ColdM	la batteria è fredda, inizia la carica di mantenimento
TxNoF	batteria al NiCd non ancora carica con telefono in trasmissione
DisCh	batteria in fase di scarica
ColdC	Carica a freddo

Questo è il menu più interessante e con il maggior numero di informazioni.

Constant voltage charging

21		21
MtDif	MpDif	- 18 0
BupV	BdownV	390 382
AverV	SumMF	390 176

MtDif	è la differenza tra la tensione misurata e quella che il telefono si aspetta di misurare.
MpDif	è la differenza tra due misurazioni successive.
BupV	Picco massimo di tensione della batteria.
BdownV	Tensione minima della batteria.
AverV	Media delle tensioni misurate.

Del menu 22 (battery status) non si sono reperite le info necessarie alla decodifica.

Battery / phone status

23			23	23
TxOn		TxOff	3466 3788	3502 3907
Chcur		StBy	0 3777	463 3778
Age	Cap	Curr	0 50 34	0 75 51
Tmp	CmA	Targ	27 61 226	27 71 286
			non carica	in carica

TxOn	tensione della batteria con il telefono in trasmissione 3.466 V
TXOff	tensione della batteria con in telefono non in trasmissione 3.788 V
Chcur	corrente di carica espressa in mA
StBy	tensione della batteria con telefono in standby 3.777 V
Age	età della batteria, da nuova (0) a vecchia (100)
Cap	carica della batteria in percentuale, da 0 a 100%
Curr	corrente istantanea di carica della batteria
Tmp	solo per la batteria al litio, temperatura della batteria
CmA	Capacita già raggiunta dalla batteria, in mA
Targ	Capacita rimanente della batteria, in mA

Il menu 30 comprende alcuni parametri dei registri audio.

Il menu 34 interessa i parametri di FBUS, il connettore che abbiamo usato per collegare il pc al telefono.

Il menu 35 riporta i motivi per cui è avvenuto l'ultimo reset del software, mentre il 36 conta i reset avvenuti e i motivi che li hanno provocati, questi contatori sono mantenuti nella eeprom del telefono.

Il menu numero 40 permette di resettare i contatori di Handover se sono presenti nei menu successivi. Le procedure di Handover si occupano del trasferimento delle conversazioni da una cella ad un'altra senza interromperle, in modo che l'utente non avverta l'avvenuto trasferimento. La sequenza di reset è la solita citata più volte, MENU, NETMONITOR, 40, OK.

Il menu 41 cambia se il telefono è un modello bibanda, nelle prime due righe conta le procedure andate a buon fine (differenziandole se il salto è avvenuto da GSM a GSM o da DCS a GSM) mentre le ultime due contano le procedure non andate a buon file o abortite, quando la connessione è stata ristabilita con la cella che si era appena abbandonata.

Il menu 42 interessa solo i modelli bibanda, continuando la serie dei contatori di handover.

Finalmente qualcosa di utile! Il menu 45 permette di disabilitare e abilitare il trasmettitore del telefono, ovvero rende il telefono non usabile. La commutazione avviene tramite la solita sequenza MENU, NETMONITOR, 45, OK. Questa azione sembra pericolosa, in realtà basta ripetere la sequenza per riportare le cose come devono essere.

SIM information

51	51
Vsim Baud Sal	3 372 YES
Scond Cstop	xxxxxxxx
Pin12 PUK12	3 0 10 0
Atr FE/PE	0 0000

Vsim tensione di alimentazione della carta SIM
Baud velocità di trasmissione dei dati dal telefono alla SIM (0, 32, 64, 372 baud)
Sal stop clock allowed (YES/NO)
PIN12 tentativi consentiti a PIN1 e PIN2
PUK12 tentativi consentiti a PUK1 e PUK2
ATR contatore delle ritrasmissioni (0-9)

I menu 52 e 53 dovrebbero riportare il contenuto della SIM del telefono, rispettivamente:

loc. di mem SIM	contenuto	nome	numero del menu
31	65535	AUDio DSP 1	71
32	65535	AUDio DSP 2	72
33	0	BTS TEST	17
34	34	52 - 53	
35	35	52 - 53	
36	36	52 - 53	

In realtà il programma non ha abilitato questi menu sul mio telefono.

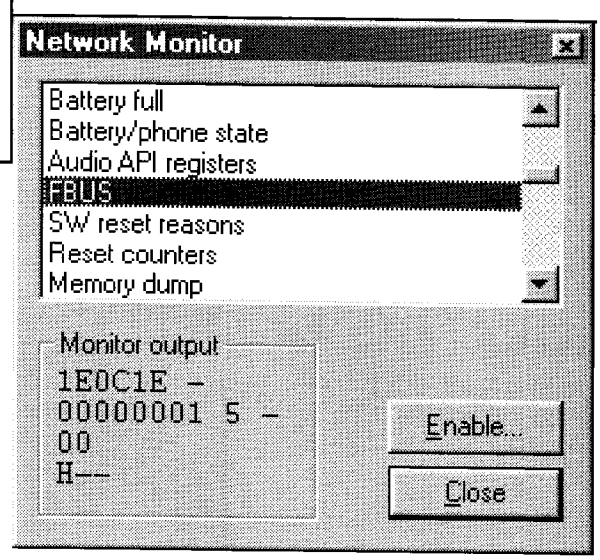
I menu 54, 55, 56 e 57 contengono posizioni di memoria e condizioni della memoria del telefono dopo un reset, probabilmente si tratta di informazioni molto importanti per la diagnostica del telefono, ma viste cosìcome le vediamo noi non significano molto.

Arriviamo finalmente alla posizione numero 60 che ci permette di resettare tutti i contatori del telefono, tramite la sequenza descritta più volte in questo testo.

I menu 61, 62, 63 e 64 riportano contatori circa le condizioni di rete, chiamate originate dal portatile, provenienti dalla rete, fino ai menu 65 e 66 che, sempre in tema di contatori si occupa di SMS.

I menu 70, 71, 72, 73, 74, 75, 76, 77, 78, 79 contengono controlli, timer e contatori circa i vari DSP presenti nel telefono. È bene notare che sul mio telefono ho solo il menù numero 75 "Audio Path Status".

Dal menu 80 riprendiamo in mano i timer, ed è quest'ultimo che permette il reset di tutti i



timer in modo del tutto analogo del menu 60 che resettava i contatori. L'abilitazione dei timer avviene tramite il menu numero 81.

Test Timer display

82 PwrOn Inserv NSPS TxOn TIMERS on/off	82 00013 00013 00000 00000 TIMERS ON

PwrOn misura il tempo da quando il telefono è acceso
Inserv misura il tempo da quando il telefono è attivo in rete
TxOn misura il tempo in cui il telefono è stato in trasmissione

Seguono i menu 83, 84, 85, 86 e 87 fino all'88 e 89 che riportano la versione del software e dell'hardware:

MCU / DSP software version

88 McusSW PPM McusSW date Mcu checksum DSP version	88 5.02 5.02A Date 990202 Chksum 0996 21. 4. 190

McusSW	versione del software
PPM	versione PPM
McusSW	date data del software nel formato AAMMGG
Mcu checksum	checksum del software
DSP version	versione del DSP

89 Hardware version Text version	89 HW: 2350 TXT: U190199

HW versione dell'hardware
TXT versione dei testi e delle lingue

Questi ultimi due menu sono simili a quanto si ottiene premendo

*#0000#

il cui risultato è:

```
V. 5.02
02-02-99
NSM-1
```

Come curiosità il numero IMEI è ricavabile dalla sequenza:

*#06#

```
N. seriale
493XXXXXXX
XXXXX
```

Queste due sequenze sono valide sia per il 5110 quanto per il 6150.

Le info necessarie alla stesura di queste pagine sono state tratte da internet, controllate sul telefono il cui contenuto del display è riportato nelle finestre di destra.

Non sono riuscito a far danni sul mio telefono, ma declino ogni responsabilità se qualcuno dovesse riuscirci! Daniele